UNE–ISO/IEC 27001: 2005 & LOPD (II)

EN ESTE NÚMERO PRESENTAMOS LA TABLA COMPLETA, EN LA CUAL SE RELACIONAN TODOS LOS ARTÍCULOS DE ESTE NUEVO REGLAMENTO

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

Carmen de Alba Muñoz

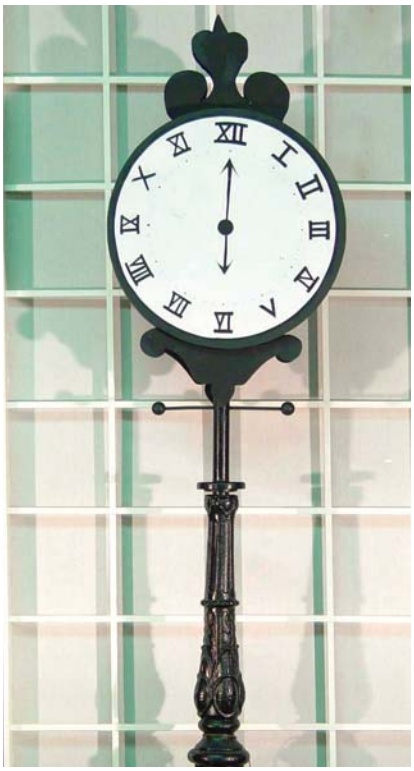
RESPONSABLE ISO-27000

NCS

En el artículo del mes pasado, hacíamos un breve repaso de los aspectos que más nos han llamado la atención del nuevo Reglamento de la LOPD. Empezamos a elaborar un cuadro, en el que relacionábamos los controles de la UNE–ISO/IEC 27001 con este reglamento, demostrando que, si se implanta un SGSI (Sistema de Gestión de la Seguridad de la Información) basándose en la norma ISO, no sólo nos aseguramos un funcionamiento eficaz de nuestros sistemas de información, sino que también cumplimos con los aspectos legales. Es decir, la UNE–ISO/IEC 27001 contempla todos los ámbitos de los sistemas de información (control de accesos, compra de equipos, alineación de los sistemas con el negocio de la compañía, cumplimiento de leyes, normas y políticas…).

En este número presentamos la tabla completa, en la cual se relacionan todos los artículos de este nuevo reglamento, con los controles de la UNE–ISO/IEC 27001, que a nuestro juicio se deben incluir o considerar, para cumplir con la LOPD, y en la columna final se establece a qué tipo de criticidad de los archivos aplica. Esta tabla es un muy elaborado resumen (y muchas horas de trabajo) de los aspectos que relacionan ambos documentos. Es decir, **si se desea afrontar cualquiera de ellos, el mejor punto de partida es esta tabla**, con la cual, lo único que queda pendiente es definir cómo medir estos controles (atributos, métricas y/o indicadores: *Ver artículo "ISO–27001 e ISO–27004")* para que cumplan con la norma y sirvan de realimentación al SGSI; no quisimos incluirlos para dejar un poco de tarea para el hogar...

> Si se realiza este trabajo a conciencia sobre esta tabla, podemos augurarles un éxito seguro



Si se realiza este trabajo a conciencia sobre esta tabla, podemos augurarles un éxito seguro, tanto en la LOPD como en el grupo 11 de UNE–ISO/IEC 27001 (Conformidades legales).

ARTÍCULO	DESCRIPCIÓN DEL REGLAMENTO	CONTROL DE LA ISO 27002	NIVEL FICH.
Doc. de Seguridad (ART. 88)	**El documento deberá contener al menos:** Ámbito de aplicación. Medidas, normas, procedimientos. Funciones y obligaciones del personal. Estructura de los ficheros y descripción de los sistemas. Medidas de transporte de soportes. Procedimientos de destrucción y reutilización. Procedimiento de notificación, gestión y respuesta ante incidencias. Procedimiento de copia de seguridad y recuperación de datos.	**5.1.1** Documento de Política de Seguridad de la Información. **10.7.2** Retirada de Soportes.	BÁSICO MEDIO ALTO
Responsable de Seguridad (ART. 95)	El Documento de Seguridad designará uno o varios Responsables de Seguridad que coordinarán las medidas definidas en el mismo. La asignación del Responsable de Seguridad puede ser única para todos los ficheros o diferenciada en función de los sistemas. Esto debe estar especificado en el Documento de Seguridad. En ningún caso, esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Fichero.	**6.1.2** Coordinación de la Seguridad de la Información. **6.1.3** Asignación de Responsabilidades Relativas a la Seguridad de la Información.	MEDIO ALTO
Funciones y Obligaciones del Personal (ART. 89)	Definición de las obligaciones y funciones de las personas con acceso a los datos. Definición de las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento. El Responsable del Fichero tomará las medidas necesarias para que todo el personal conozca las normas de seguridad que afectan al fichero.	**8.1.1** Funciones y Responsabilidades. **8.2.2** Concienciación, Formación y Capacitación en Seguridad de la Información. **8.2.3** Proceso Disciplinario.	BÁSICO MEDIO ALTO
Registro de Incidencias (ART. 90)	Procedimiento de notificación y gestión de incidencias con un registro con los siguientes campos: ■ Tipo de incidencias. ■ Momento en el que se ha producido. ■ Persona que lo notifica. ■ A quien se lo notifica. ■ Efectos de la incidencia. ■ Medidas correctoras aplicadas.	**12.6.1** Control de las Vulnerabilidades Técnicas. **13.1.1** Notificación de los Eventos de Seguridad de la Información. **13.2.1** Responsabilidades y Procedimientos. **13.2.2** Aprendizaje de los Incidentes de Seguridad. **13.2.3** Recopilación de Evidencias.	BÁSICO MEDIO ALTO
Registro de Incidencias (ART. 100)	Además, el Procedimiento de notificación y gestión de incidencias debe contener: ■ Procedimientos realizados para la recuperación de los datos. ■ Persona que ha ejecutado el proceso. ■ Datos Restaurados. ■ Datos que se han grabado manualmente. ■ Autorización por escrito del Responsable del Fichero para recuperar los datos.	**13.1.1** Notificación de los Eventos de Seguridad de la Información. **13.2.1** Responsabilidades y Procedimientos. **13.2.2** Aprendizaje de los Incidentes de Seguridad. **13.2.3** Recopilación de Evidencias.	MEDIO ALTO

ARTÍCULO	DESCRIPCIÓN DEL REGLAMENTO	CONTROL DE LA ISO 27002	NIVEL FICH.
Control del Acceso (ART. 91)	Los usuarios acceden a los recursos necesarios para desempeñar su trabajo. El Responsable del Fichero elaborará una relación actualizada de usuarios, perfiles y permisos de acceso. El Responsable del Fichero establece mecanismos para evitar que los usuarios accedan a recursos no autorizados. El personal autorizado en el Documento de Seguridad tiene la potestad para conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme al criterio establecido por el Responsable del Fichero. El personal ajeno al responsable del fichero que tenga acceso a los datos está sometido a las mismas condiciones y obligaciones de seguridad que el resto del personal.	**6.1.5** Acuerdos de Confidencialidad. **6.2.3** Tratamiento de la Seguridad en Contratos con Terceros. **9.1.2** Controles Físicos de Entrada. **10.8.2** Acuerdos de Intercambio. **11.1.1** Política de Control de Acceso. **11.2.1** Registro de Usuario. **11.2.2** Gestión de Privilegios. **11.2.3** Gestión de Contraseñas de Usuario. **11.2.4** Revisión de los Derechos de Acceso de Usuario. **11.6.1** Restricción del Acceso a la Información. **13.2.1** Responsabilidades y Procedimientos.	BÁSICO MEDIO ALTO
Control de Acceso Físico (ART. 99)	El personal autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se encuentren ubicados los Sistemas de Información.	**9.1.1** Perímetro de Seguridad Física. **9.1.2** Controles Físicos de Entrada.	MEDIO ALTO
Registro de Accesos (ART. 103)	De cada acceso se almacenará como mínimo: ■ ID del usuario. ■ Fecha y hora. ■ Fichero accedido. ■ Tipo de acceso. ■ Si el acceso ha sido autorizado o denegando. Si el acceso ha sido autorizado, se debe almacenar a información que identifique el registro accedido. Los mecanismos que permiten el registro de los datos detallados en los puntos anteriores son controlados directamente por el Responsable de Seguridad, no permitiéndose en todo caso, la desactivación de los mismos. El periodo mínimo de conservación de los datos es de 2 años. El Responsable de Seguridad competente debe encargarse de revisar periódicamente la información de control registrada, elaborando un informe de las revisiones realizadas y los problemas detectados, al menos una vez al mes. El Registro de Accesos no será necesario si: ■ El Responsable del Fichero o del Tratamiento es una persona física. ■ El Responsable del Fichero o del Tratamiento garantiza que él es el único que tiene acceso y trata los datos. Si se da este caso, deberá estar especificado en el Documento de Seguridad.	**11.1.1** Política de Control de Acceso. **11.2.1** Registro de Usuario. **11.2.2** Gestión de Privilegios. **11.2.4** Revisión de los Derechos de Acceso de Usuario.	ALTO
Gestión de Soportes y Documentos (ART. 92)	Los soportes informáticos que contengan datos de carácter personal deben: ■ Permitir identificar el tipo de información que contienen. ■ Ser inventariados. ■ Almacenarse en un lugar seguro con acceso restringido al personal autorizado.	**7.2.1** Directrices de Clasificación. **7.2.2** Etiquetado y Manipulado de la Información. **9.1.2** Controles Físicos de Entrada. **9.1.4** Protección Contra las Amenazas Externas y de Origen Ambiental.	BÁSICO MEDIO ALTO

ARTÍCULO	DESCRIPCIÓN DEL REGLAMENTO	CONTROL DE LA ISO 27002	NIVEL FICH.
Gestión de Soportes y Documentos (ART. 92)	La salida de soportes fuera de los locales sólo podrá ser autorizada por el Responsable del Fichero o debidamente autorizada en el Documento de Seguridad. Aplicar las medidas necesarias para evitar pérdidas, robos o accesos no autorizados durante su transporte. Cuando se vaya a desechar o destruir un soporte, se deben adoptar las medidas oportunas para evitar que se pueda recuperar o acceder a la información.	**9.2.6** Reutilización o Retirada Segura de los Equipos. **10.8.1** Políticas y Procedimientos de Intercambio de Información. **10.8.3** Soportes Físicos en Tránsito. **10.8.5** Sistemas de Información Empresariales. **11.6.1** Restricción del Acceso a la Información.	
Gestión de Soportes y Documentos (ART. 97)	Se debe establecer un sistema de **Registro de Entrada** de soportes informáticos que permita directa o indirectamente conocer: ■ Tipo de soporte. ■ Fecha y hora. ■ El emisor. ■ El número de soportes recibidos. ■ El tipo de información que contiene. ■ La forma de envío. ■ La persona responsable de la recepción (debe estar autorizada para ello). Se debe establecer un sistema de **Registro de Salida** de soportes informáticos que permita directa o indirectamente conocer: ■ Tipo de soporte. ■ Fecha y hora. ■ El destinatario. ■ El número de soportes enviados. ■ El tipo de información que contiene. ■ La forma de envío. ■ La persona responsable de la entrega (debe estar autorizada para ello).	**10.8.1** Políticas y Procedimientos de Intercambio de Información.	MEDIO ALTO
Identificación y Autenticación (ART. 93)	Mecanismo que permita la identificación de forma inequívoca y personalizada de los usuarios que accedan al sistema, y la verificación de que está autorizado. Procedimiento de asignación, distribución y almacenamiento de contraseñas. Procedimiento de cambio de contraseñas de forma periódica. Almacenamiento de las contraseñas de forma intangible.	**11.2.1** Registro de Usuario. **11.2.3** Gestión de Contraseñas de Usuario. **11.2.4** Revisión de los Derechos de Acceso de Usuario. **11.5.2** Identificación y Autenticación de Usuario. **11.5.3** Sistema de Gestión de Contraseñas.	BÁSICO MEDIO ALTO
Identificación y Autenticación (ART. 98)	Se establecerá un mecanismo para limitar el número de intentos de acceso al sistema.	**11.1.1** Política de Control de Acceso. **11.5.1** Procedimientos Seguros de Inicio de Sesión.	ALTO
Copias de Respaldo y Recuperación (ART. 94)	Se deben realizar copias de respaldo al menos semanalmente, salvo que en dicho periodo no se haya producido ninguna actualización de los datos.		

ARTÍCULO	DESCRIPCIÓN DEL REGLAMENTO	CONTROL DE LA ISO 27002	NIVEL FICH.
Copias de Respaldo y Recuperación (ART. 94)	Los procedimientos deben garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Documento de Seguridad. El Responsable del Fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de las copias de respaldo y recuperación de datos. Las pruebas anteriores a la implantación o modificación del sistema no se realizarán con datos reales, salvo que se asegure su nivel de seguridad y sea anotado en el Documento de Seguridad.Antes de realizar una prueba con datos reales ha de hacerse una copia de seguridad.	**10.5.1** Copias de Seguridad de la Información. **10.7.3** Procedimientos de Manipulación de la Información. **12.4.2** Protección de los Datos de Prueba del Sistema.	BÁSICO MEDIO ALTO
Copias de Respaldo y Recuperación (ART. 102)	Antes probar con datos reales ha de hacerse una copia de seguridad. Se debe conservar una copia de respaldo y los procedimientos de recuperación de datos en un lugar diferente de aquél en que se encuentran los equipos informáticos que los tratan, cumpliendo siempre las medidas de seguridad exigidas.	**10.5.1** Copias de Seguridad de la Información. **10.7.1** Gestión de Soportes Extraíbles. **10.7.2** Retirada de Soportes.	ALTO
Auditoría (ART. 96)	Los SSII e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa al menos cada 2 años que verifique: ■ El cumplimiento del Reglamento. ■ Los procedimientos e instrucciones vigentes en materia de seguridad de datos. Con carácter extraordinario se realizará una auditoría si se han realizado cambios en el sistema que afecten al cumplimiento de las medidas de seguridad implantadas. El informe de auditoría debe dictaminar sobre: ■ La adecuación de las medidas y controles a la Ley. ■ Identificar sus deficiencias. ■ Proponer medidas correctoras o complementarias. ■ Incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas. Los informes de auditoría los analizará el Responsable de Seguridad competente, que elevará las conclusiones al Responsable del Fichero para adoptar las medidas correctoras adecuadas, y quedarán a disposición de la AGPD o a las autoridades de control de las comunidades autónomas.	**6.1.6** Contacto con las Autoridades. **6.1.8** Revisión Independiente de la Seguridad de la Información. **10.10.1** Registro de Auditorías. **10.10.2** Seguimiento del Uso del Sistema. **10.10.5** Registro de Fallos.	MEDIO ALTO
Telecomunicaciones (ART. 104)	La transmisión de datos a través de redes públicas o redes inalámbricas de comunicaciones de datos, se realizarán cifrando dichos datos, o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.	**12.3.1** Política de Uso de los Controles Criptográficos. **12.3.2** Gestión de Claves.	ALTO